GRUPO DE PESQUISA EM

DESAFIOS DA PROTEÇÃO DE DADOS E INTELIGÊNCIA ARTIFICIAL

ANALÍTICOS

JUS SCRIPTUM'S
INTERNATIONAL JOURNAL OF LAW
a. 20 • v. 10 • dossiê • 2025

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA
Associação Académica da Faculdade de Direito de Lisboa
AAFDL
nelb

JUS SCRIPTUM'S
INTERNATIONAL JOURNAL OF LAW
REVISTA INTERNACIONAL DE DIREITO

DESAFIOS DA PROTEÇÃO DE DADOS E INTELIGÊNCIA ARTIFICIAL

Analíticos do Grupo de Pesquisa em
Proteção de Dados e Inteligência Artificial

Núcleo de Estudo Luso-Brasileiro
Faculdade de Direito da Universidade de Lisboa

2025
a. 20 v. 10 d. 1
EDIÇÃO ESPECIAL

Jus Scriptum's International Journal of Law
Revista Internacional de Direito do Núcleo de Estudo Luso-Brasileiro da Faculdade de Direito da Universidade de Lisboa
Ano 20 • Volume 10 • Edição Especial • 2025
Analíticos do Grupo de Pesquisa em Proteção de Dados e Inteligência Artificial

Periodicidade Trimestral
ISSN 1645-9024

Equipe Editorial

Corpo de Avaliadores – Peer Review Board

Anjuli Tostes Faria Melo
Camila Franco Henriques
Carla Valério
Caroline Lima Ferraz
César Fiuza
Eduardo Alvares de Oliveira
Francine Pinto da Silva Joseph
Isaac Kofi Medeiros
J. Eduardo Amorim
José Antonio Cordeiro de Oliveira
Leonardo Bruno Pereira de Moraes
Leonardo Castro de Bone
Marcelo Ribeiro de Oliveira
Marcial Duarte de Sá Filho
Maria Vitoria Galvan Momo
Plínio Régis Baima de Almeida
Rafael Vasconcellos de Araújo Pereira
Rafaela Câmara Silva
Renato Sedano Onofre
Silvia Gabriel Teixeira
Thais Cirne
Vânia dos Santos Simões

Grupo de Pesquisa em Proteção de Dados e Inteligência Artificial

Profa. Doutor Mariana Moraes Palmeira, Coordenadora Científica
Dr. Daniel Serrão, Coordenador Executivo

Alessandra Fonseca de Carvalho;
Aline Pinheiro;
Ana Cristina Oliveira Mahle;
Anna Carolina Almeida da Cruz;
Camila Franzo;
Carlos Mendes da Silveira Cunha;
Carolina Tavares Vieira Félix;
Cláudio Cardona;
Claudio Roberto Sales Kistler Junior;
Cristiane Rafaela Dallastra;
Dânton Zanetti;
Francisco Soares Reis Júnior;
Gabriela Cristine Buzzi;
Jade Caldas Sibalde;
Joice Bernardo do Carmo;
Júlia Castro John;
Lorena Garrido Borges;
Lucas Azoubel;
Maria Vitória Galvan Momo;
Mariana Fernandes Conrado;
Marina Goulart de Queiroz;
Patrícia Ferreira de Almeida;
Sharlynn Margery De Jongh Martins;
Thiago de Araújo Carneiro Leão;
Wilson Furtado Roberto.

DARK PATTERNS E NEURODIREITOS: PROTEÇÃO DA PRIVACIDADE E DESAFIOS REGULATÓRIOS NO CONTEXTO DIGITAL

Dark patterns and neurorights: privacy protection and regulatory challenges in the digital context

Ana Cristina Oliveira Mahle[†]

Este artigo examina os impactos dos dark patterns na privacidade dos usuários, com foco nas regulamentações europeias e brasileiras, incluindo o GDPR e a LGPD. Os dark patterns são estratégias de design de interface que manipulam os usuários, levando-os a tomar decisões contrárias aos seus melhores interesses. O estudo explora a aplicação dessas práticas no contexto de dados sensíveis e de vulneráveis, como crianças e adolescentes, além de discutir a interseção entre dark patterns e neurodireitos. O artigo também analisa como as neurotecnologias emergentes, como interfaces cérebro-computador e implantes neurais, podem ser impactadas por práticas de design manipulativas, destacando a importância de regulamentações que protejam a integridade mental e a privacidade dos indivíduos.

Palavras-chave: Dark Patterns, Neurodireitos, Privacidade, Proteção de Dados, LGPD, GDPR, Consumidor Vulnerável.

This article examines the impacts of dark patterns on user privacy, focusing on European and Brazilian regulations, including the GDPR and LGPD. Dark patterns are interface design strategies that manipulate users into making decisions against their best interests. The study explores the application of these practices in the context of sensitive and vulnerable data, such as that of children and adolescents, and discusses the intersection between dark

[†] Advogada, mestre e doutoranda em Ciência, Tecnologia e Sociedade pela UFSCar, com pesquisa em proteção de dados e inteligência artificial. Associada ao escritório Moore Prisma, em Ribeirão Preto/SP, com atuação em DPO as a Service e consultoria em LGPD e ESG. Coordenadora da Comissão de Privacidade e Proteção de Dados da 87ª Subseção da OAB/SP desde agosto de 2020, ex-Coordenadora da Comissão da Mulher Advogada e DPO Setorial da 87ª Subseção, integrando o Comitê de Governança de Dados e Segurança da Informação desde novembro de 2022. Possui experiência docente em cursos e oficinas jurídicas, incluindo formação ofertada pela ESA com elevada procura em 2022. É bacharela em Direito pela UNIP, mestre e doutoranda pela UFSCar e cursa pós-graduação em Compliance, Governança Corporativa e ESG pela Damásio. É autora de artigos e capítulos sobre direito digital e proteção de dados e possui certificações e cursos de extensão em privacidade, incluindo certificação pelo Data Privacy Brasil.

patterns and neuro-rights. The article also analyzes how emerging neurotechnologies, such as brain-computer interfaces and neural implants, may be affected by manipulative design practices, highlighting the importance of regulations that protect individuals' mental integrity and privacy.

Keywords: Dark Patterns, Neuro-rights, Privacy, Data Protection, LGPD, GDPR, Vulnerable Consumers.

1. Introdução

Na atualidade, a proteção de dados pessoais tornou-se uma preocupação central para os governos, organizações e indivíduos. Com o crescimento exponencial do uso de tecnologias digitais e a proliferação de dispositivos conectados, a quantidade de dados pessoais coletados, armazenados e processados atingiu níveis sem precedentes. Este cenário trouxe à tona novos desafios e ameaças à privacidade dos usuários, incluindo a emergência dos chamados "*dark patterns*"[1].

Em uma época em que as *fakes news* são prevalentes, o conceito de "*dark patterns*" ou também conhecidos como "padrões de *design* enganosos" ou mesmo "padrões obscuros", tem se tornado cada vez mais relevante. Esse termo tem se tornado cada vez mais conhecido e discutido ao redor do mundo.

Esse conceito foi introduzido em 2010 por Harry Brignull[2], um *design*er de UX britânico, que criou um *website* dedicado ao tema. Ele descreve esses padrões como *Deceptive Patterns* ou *design* enganoso que é um termo sinônimo.

[1]Brignull, Harry. "Dark Patterns: Deception vs. Honesty in UI *Design"*. 2011. https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/
[2] Brignull,. "Dark Patterns".

Um *design*er de UX, ou experiência do usuário (*user experience*), é responsável por criar interfaces de usuário que são intuitivas, acessíveis e que proporcionam uma experiência agradável aos usuários. O trabalho de um *design*er de UX envolve pesquisa sobre os usuários, criação de *wireframe*s, protótipos, testes de usabilidade e ajustes com base no *feedback* dos usuários para garantir que o produto final atenda às necessidades e expectativas do público-alvo. Foi através dessa prática de compreender as interações entre usuários e interfaces que Harry Brignull[3] identificou a presença de padrões de *design* enganosos.

Esses padrões se referem a *designs* de interface que tentam enganar, coagir ou pressionar os usuários a realizar ações específicas, como compras ou inscrições. As táticas utilizadas nesses *designs* podem incluir vantagens desiguais nas opções disponíveis ou até declarações falsas, enganosas ou ocultas, levando os usuários a tomarem decisões inadequadas ou adotarem comportamentos que vão contra as leis de proteção de dados pessoais.

Esses padrões são mais comuns do que se imagina e são frequentemente praticados por grandes empresas, tanto nacionais quanto multinacionais. Por exemplo, um site pode apresentar um *pop-up* de consentimento com um botão que diz "Aceitar todos os cookies", sem oferecer ao usuário a opção de rejeitar ou escolher quais cookies aceitar[4].

[3] Brignull, “Dark Patterns”.
[4] “Dark patterns in data protection,” Lickslegal, 2023, https://www.lickslegal.com/post/dark-patterns-in-data-protection

Outro exemplo comum em sites de notícias e revistas é a publicidade paga disfarçada de conteúdo editorial, utilizando características falsas ou enganosas para impulsionar as vendas de um produto específico.

Para além das práticas enganosas que afetam o público em geral, é importante ressaltar que crianças e adolescentes constituem um grupo especialmente vulnerável às estratégias de *dark patterns*. De acordo com a LGPD[5], o tratamento de dados pessoais desse grupo deve observar o "melhor interesse" da criança, exigindo um consentimento específico dado por pelo menos um dos pais ou responsável legal. No entanto, as táticas manipulativas de *design* podem facilmente explorar a falta de experiência e entendimento das crianças, levando-as a tomar decisões prejudiciais sem a devida compreensão das consequências[6]. Como resultado, esses jovens podem ser levados a fornecer dados pessoais ou realizar ações que comprometem sua privacidade, sem a intervenção adequada de seus responsáveis[7].

O uso de *dark patterns* em plataformas voltadas para crianças e adolescentes é particularmente preocupante porque esses usuários, muitas vezes, não possuem a capacidade cognitiva para distinguir entre uma interface amigável e uma manipulativa. Conforme destacado por Brandão[8], crianças entre 3 e 7 anos, por exemplo, têm dificuldade em compreender motivações persuasivas e podem não

[5] "Lei nº 13.709, de 14 de Agosto de 2018 (Lei Geral de Proteção de Dados Pessoais)." Diário Oficial da União, 15 de agosto de 2018, seção 1, p. 53-58

[6] Brandão, Renan Sancho. "Tratamento de dados pessoais de crianças e adolescentes: análises e perspectivas." (Monografia, Universidade Federal do Rio de Janeiro, 2022), https://pantheon.ufrj.br/handle/11422/19142

[7] Henriques, Isabella Vieira Machado, Inês Vitorino Sampaio. "Discriminação algorítmica e inclusão em Sistemas de Inteligência Artificial – uma reflexão sob a ótica dos direitos da criança no ambiente digital". *RDB*, Brasília, 18, no. 100 (out. dez. 2021): 245-271. https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5993/pdf

[8] Brandão, "Tratamento de dados pessoais"

reconhecer uma mensagem publicitária, tornando-as suscetíveis a influências externas que as incentivem a compartilhar dados pessoais ou realizar compras dentro de aplicativos. Isso gera uma necessidade urgente de regulamentação e fiscalização para proteger esse público, garantindo que as interações digitais sejam feitas de forma ética e segura[9].

Além disso, a prática de *dark patterns* pode ter efeitos de longo prazo no desenvolvimento de crianças e adolescentes. Quando expostos repetidamente a essas práticas, eles podem desenvolver comportamentos de consumo impulsivos e dependentes, influenciados por interfaces que priorizam o lucro das empresas em detrimento da proteção dos dados pessoais e da saúde mental dos jovens[10]. Isso é agravado pelo fato de que adolescentes, em especial, são suscetíveis a pressões externas e buscam aprovação social, o que pode ser explorado por padrões de *design* enganosos para incentivá-los a compartilhar mais informações pessoais ou a gastar dinheiro em produtos ou serviços que não necessitam[11]. Como consequência, a autonomia informativa e o direito à privacidade desses jovens são seriamente comprometidos[12].

A gravidade dessa situação foi recentemente evidenciada no processo movido pela cidade de Nova York contra várias redes sociais, como TikTok, Instagram, Facebook, Snapchat e YouTube, alegando que os *design*s dessas plataformas

[9] Eberlin, Fernando Büscher von Teschenhausen. "Proteção de dados pessoais da criança: privacidade, vulnerabilidade e consentimento na sociedade da informação." Dissertação de Mestrado, Universidade Presbiteriana Mackenzie, 2019. https://bdtd.ibict.br/vufind/Record/UPM_27ce6ed381aa9f5fb0a3fd2e271e3ffa
[10] Henriques, Machado, "Discriminação algorítmica".
[11] Eberlin, "Proteção de dados pessoais".
[12] Brandão, "Tratamento de dados pessoais".

exploram a saúde mental dos jovens, contribuindo para uma crise de saúde pública. O processo alega que essas plataformas são responsáveis por um aumento significativo nos problemas de saúde mental entre os jovens, incluindo depressão e transtornos suicidas, e impõem um grande fardo financeiro aos sistemas de saúde e educação da cidade, que gastam anualmente cerca de US$ 100 milhões em programas e serviços relacionados[13].

Este caso também chama a atenção para o impacto das redes sociais no bem-estar dos jovens, especialmente no que diz respeito às características "viciantes" e "perigosas" das plataformas, que podem substituir interações sociais saudáveis por comportamentos digitais prejudiciais. Embora as empresas tenham defendido suas plataformas e afirmado que estão comprometidas com a segurança dos jovens, a cidade de Nova York busca responsabilizá-las por seu papel na crise de saúde mental, pedindo compensação financeira e exigindo medidas preventivas mais rigorosas. Esse movimento se alinha a iniciativas regulatórias mais fortes, como as previstas na União Europeia, onde as empresas podem ser processadas por violar a Lei dos Serviços Digitais (EUA), enfrentando multas de até 6% de suas receitas globais[14].

Portanto, é crucial que haja uma ação coordenada entre reguladores, educadores e desenvolvedores de tecnologia para combater o uso de padrões de *design* enganosos, especialmente em interfaces direcionadas a crianças e adolescentes. A implementação de práticas como o *privacy by design* e a adoção de medidas éticas

[13] Kelly, Samantha Murphy. “Nova York processa redes sociais por crise de saúde mental de adolescentes.” CNN Brasil, 2024. https://www.cnnbrasil.com.br/economia/negocios/nova-york-processa-redes-sociais-por-crise-de-saude-mental-de-adolescentes/
[14] Kelly, “Nova York processa redes sociais.”

e de transparência são passos fundamentais para garantir que as plataformas digitais respeitem os direitos dos usuários mais jovens. A sociedade precisa reconhecer que a proteção desse grupo vulnerável exige não apenas o cumprimento das leis de proteção de dados, mas também uma ética de *design* que priorize o bem-estar e o desenvolvimento saudável das crianças e adolescentes no ambiente digital[15] [16].

Essa proteção contra padrões de *design* enganosos é extremamente necessária não apenas para proteger esse grupo vulnerável, mas também para a sociedade como um todo, já que *dark patterns* podem causar sérios danos até mesmo entre adultos. Por exemplo, práticas como a inscrição automática em assinaturas recorrentes sem o devido consentimento ou a apresentação de opções desiguais em *pop-ups* de cookies podem levar consumidores a decisões financeiras prejudiciais ou à exposição inadvertida de seus dados pessoais. Estudos mostram que mesmo usuários adultos, quando submetidos a essas táticas manipulativas, podem acabar gastando dinheiro em produtos ou serviços indesejados, ou compartilhando mais informações do que pretendiam originalmente, o que compromete sua privacidade e segurança[17] [18].

Diante do exposto, entende-se que a prática de *Dark patterns* ocorre através de estratégias de *design* de interface deliberadamente enganosas, criadas para manipular os usuários a realizar ações que muitas vezes comprometem sua privacidade e segurança. Esses padrões obscurecem informações, dificultam a navegação por

[15] Henriques, Machado, “Discriminação algorítmica”.
[16] Eberlin, “Proteção de dados pessoais”.
[17] Henriques, Machado, “Discriminação algorítmica”.
[18] Eberlin, “Proteção de dados pessoais”.

opções de privacidade e incentivam a tomada de decisões que beneficiam os provedores de serviços em detrimento dos direitos dos usuários[19].

Ainda, nesse sentido, *dark patterns*, ou padrões obscuros, induzem os usuários a tomar decisões que eles não teriam tomado de outra forma, muitas vezes prejudicando seus interesses. Brignull[20], define *dark patterns* como interfaces que foram cuidadosamente elaboradas para enganar ou coagir usuários a fazer escolhas que, de outra forma, eles não fariam[21]. Exemplos comuns de *dark patterns* incluem:

Privacy Zuckering: Manipulação para que os usuários compartilhem mais dados pessoais do que gostariam[22]. *Privacy Zuckering* é uma prática enganosa que esconde informações e pode ser assimétrica, focando na receita adicional de publicidade ou corretagem de dados. Este *dark pattern* aparece em políticas de privacidade e termos de condições ao se inscrever em plataformas ou serviços, usando técnicas que induzem os usuários a revelarem mais informações do que pretendiam. As plataformas atuam como corretores de dados, vendendo essas informações para empresas que as utilizam para direcionamento de anúncios. Este padrão é frequentemente disfarçado em termos de uso e políticas de privacidade longas e complexas. Pode-se tomar como exemplo as gigantes Facebook e Google, elas fornecem serviços gratuitos, mas monetizam os dados dos usuários. Em um relatório da NCC de

[19] Gray, Colin M., Yubo Kou, Bryan Battles, Joseph Hoggatt, & Autin L. (2018). "The dark (patterns) side of UX *design*." Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 534.
[20] Brignull,. "Dark Patterns".
[21] Brignull,. "Dark Patterns".
[22] Bösch, Christoph, Benjamin Erb, Frank Kargl, Henning Kopp & Stefan Pfattheicher. "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns." Proceedings on Privacy Enhancing Technologies, 2016(4), 237-254. https://www.researchgate.net/publication/303814886_Tales_from_the_Dark_Side_Privacy_Dark_Strategies_and_Privacy_Dark_Patterns

2018, ambas foram acusadas de oferecer uma "ilusão de controle" através de métodos como esconder opções de privacidade, escolhas "tudo ou nada", e arquiteturas de escolha que dificultam a seleção de opções amigáveis à privacidade. O relatório detalha como essas empresas utilizam práticas exploratórias para induzir os usuários a divulgarem mais dados do que fariam normalmente[23].

Hidden Legalese Stipulations: envolvem esconder termos e condições importantes em documentos longos e complexos, escritos em linguagem jurídica difícil de entender. Isso torna difícil para os usuários compreenderem completamente a que estão consentindo. As empresas muitas vezes aproveitam essa complexidade para incluir cláusulas que lhes permitem coletar e utilizar dados de maneiras que os usuários não aprovariam se entendessem plenamente os termos[24].

Forced Registration: é a prática de exigir que os usuários criem uma conta para acessar conteúdos ou serviços que deveriam ser acessíveis sem essa necessidade. Isso não só cria uma barreira de entrada desnecessária, mas também força os usuários a fornecer informações pessoais que podem ser utilizadas para fins de *marketing* e outras práticas comerciais[25]. Esse padrão é comum em sites de e-commerce e plataformas de mídia social. A proteção de dados na era digital é de extrema importância, pois os dados pessoais são frequentemente utilizados para diversos fins,

[23] Mazumdar, Stuti & Symran Bhue. “Responsible design part 10 of 14 : privacy zuckering.” Thing Design, 2022. https://think.*design*/blog/responsible-*design*-part-10-of-14-privacy-zuckering/#:~:text=Privacy%20Zuckering%20is%20a%20dark,the%20users%20had%20intended%20to

[24] Luguri, Jamie, & Lior Jacob Strahilevitz. “Shining a Light on Dark Patterns”. Journal of Legal Analysis, 13, 43-109, 2023.

[25] Mathur, Arunesh, Gunes Acar, Michael Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, & ArvindNarayanan, A. (2019). “Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites”. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 81, 2019. https://dl.acm.org/doi/10.1145/3359183

incluindo *marketing* direcionado, desenvolvimento de produtos e serviços, e até manipulação de comportamento. A violação de privacidade pode levar a sérias consequências, como roubo de identidade, discriminação e perda de confiança dos consumidores[26].

O histórico dos *dark patterns* está intimamente ligado ao crescimento da economia digital e ao aumento da coleta de dados pessoais. À medida que as empresas começaram a depender cada vez mais dos dados dos usuários para direcionamento de anúncios e outras práticas comerciais, as técnicas de *design* manipulativas se tornaram comuns. Estudos mostram que essas práticas não apenas violam a privacidade dos usuários, mas também podem causar danos psicológicos e financeiros[27] [28].

O impacto dos *dark patterns* nos usuários pode ser significativo e multifacetado. Primeiramente, essas práticas comprometem a privacidade dos usuários, expondo-os a riscos como roubo de identidade e discriminação. Além disso, padrões de *design* enganosos podem levar a decisões financeiras prejudiciais, como a compra de produtos indesejados ou a inscrição em serviços pagos inadvertidamente[29].

Estudos mostram que a exposição contínua aos *dark patterns* pode resultar em desgaste psicológico, levando a uma redução na confiança nas plataformas

[26] Acquisti, Alessandro, Laura Brandimarte & George Loewenstein. "Privacy and human behavior in the age of information." Science, 347(6221), 509-514, 2015.
[27] Gray, Colin M., Yubo Kou, Bryan Battles, Joseph Hoggatt, & Autin L. (2018). "The dark (patterns) side of UX *design*." Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 534.
[28] Bösch et al. "Tales from the Dark Side".
[29] Acquisti, Brandimarte & Loewenstein, "Privacy and human behavior".

digitais e aumentando a ansiedade em relação à privacidade e segurança *online*[30]. A manipulação persistente também pode impactar a autonomia dos usuários, interferindo em sua capacidade de tomar decisões informadas e voluntárias[31].

A interseção entre *dark patterns* e neurodireitos ocorre quando as estratégias de *design* manipulativas não só influenciam decisões de compra ou uso de serviços, mas também interferem diretamente nos processos mentais dos usuários. Neurotecnologias, como interfaces cérebro-computador (BCIs), têm a capacidade de acessar e modificar dados neurais, expondo os indivíduos a novas formas de manipulação. Quando combinadas com *design* enganosos, essas tecnologias podem ser utilizadas para influenciar sub-repticiamente os pensamentos, emoções e comportamentos dos usuários, levantando sérias preocupações sobre a violação da autonomia mental e da privacidade[32].

Um exemplo dessa interseção pode ser encontrado no uso de *hypernudging*, que são formas avançadas de manipulação computacional. *Hypernudges* utilizam grandes quantidades de dados para adaptar continuamente a experiência do usuário de maneira a influenciar suas decisões de forma imperceptível. Isso é particularmente problemático no contexto das neurotecnologias, onde as informações obtidas podem ser usadas para criar perfis psicológicos detalhados e prever ou até mesmo influenciar o comportamento futuro dos indivíduos. A manipulação dessa natureza

[30] Gray, Kou, Battles, Hoggatt, & Autin. "The dark (patterns) side of UX *design*."
[31] Faraoni, Stefano. "Persuasive Technology and Computational Manipulation: Hypernudging out of Mental Self-Determination." Frontiers in Artificial Intelligence, 6, 2023. https://doi.org/10.3389/frai.2023.1216340
[32] Orias, Ramiro. "Los neuroderechos: una nueva Frontera para los Derechos Humanos." Agenda Internacional, Año XXIX, no. 40, 2022, 211-227. https://revistas.pucp.edu.pe/index.php/agendainternacional/article/view/26019/24500

compromete a capacidade dos indivíduos de tomar decisões informadas e voluntárias, violando assim seus neurodireitos fundamentais[33].

Além disso, a coleta e utilização de dados neurais por meio de *dark patterns* podem levar a discriminação e exclusão social. Por exemplo, algoritmos de publicidade que utilizam dados neurais podem segmentar usuários com base em suas vulnerabilidades emocionais ou cognitivas, promovendo produtos ou serviços que exploram essas fraquezas. Essa prática não só compromete a privacidade dos indivíduos, mas também pode resultar em impactos negativos em sua saúde mental e bem-estar. Fica evidente a necessidade de um olhar de cautela entre a intersecção de *dark patterns* e neurodireitos, pois sem proteções adequadas, os indivíduos ficam expostos a formas invasivas e potencialmente prejudiciais de manipulação digital[34] [35].

A União Europeia, por meio do Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* - GDPR), estabeleceu um marco na proteção de dados pessoais, impondo regras rigorosas sobre como as empresas devem coletar, armazenar e processar informações pessoais. No Brasil, a Lei Geral de Proteção de Dados (LGPD) segue a mesma linha, buscando assegurar os direitos dos cidadãos em relação aos seus dados pessoais e promover práticas transparentes e seguras no manejo dessas informações[36].

---

[33] Acquisti, Brandimarte & Loewenstein, "Privacy and human behavior".
[34] Gray, Kou, Battles, Hoggatt, & Autin. "The dark (patterns) side of UX *design*."
[35] Bösch et al. "Tales from the Dark Side".
[36] Palmeira, Mariana de Moraes. "UX: entre o Marketing e a Lei Geral de Proteção de Dados (LGPD)." Observatório da Comunicação, 2020. https://observatoriodacomunicacao.org.br/artigos/ux-entre-o-marketing-e-a-lei-geral-de-protecao-de-dados-lgpd-por-mariana-de-moraes-palmeira/

Desse modo, o objetivo do presente artigo é analisar os impactos dos *dark patterns* na privacidade dos usuários, comparando as regulamentações dessas práticas entre a Europa e o Brasil, além de explorar a interseção entre essas práticas de *design* enganosas e os neurodireitos, com ênfase na proteção de dados sensíveis e na eficácia das regulamentações existentes.

2. Neurodireitos e privacidade

Os neurodireitos representam uma nova categoria de direitos humanos, concebidos para proteger a atividade cerebral e a integridade mental dos indivíduos em face das tecnologias emergentes, como as neurotecnologias. Propostos inicialmente pelo neurocientista Rafael Yuste, os neurodireitos incluem cinco categorias principais: direito à privacidade mental, direito à identidade pessoal, direito ao livre arbítrio, direito ao acesso equitativo desse aprimoramento cognitivo e proteção contra preconceitos e informações mal-intencionadas (vieses)[37].

Nesse entendimento, Ienca e Andorno[38] propõem a introdução de quatro direitos fundamentais na era da neurotecnologia: direito à privacidade cognitiva, direito à integridade psicológica, direito à autonomia mental e direito à proteção contra viés algorítmico e discriminação. Esses direitos são descritos da seguinte forma:

- Direito à Privacidade Cognitiva: Este direito protege os indivíduos contra o acesso não autorizado aos seus dados cerebrais. Os autores enfatizam a

[37] Orias, “Los neuroderechos”
[38] Ienca, Marcello; Roberto Andorno. “Towards new human rights in the age of neuroscience and neurotechnology.” Life Sciences, Society and Policy, 13, no. 5, 2017. https://link.springer.com/article/10.1186/s40504-017-0050-1

importância de salvaguardar informações neurológicas, que podem revelar pensamentos, intenções e sentimentos, contra interceptações e análises não consentidas.

- Direito à Integridade Psicológica: Este direito garante que os indivíduos não sejam submetidos a alterações coercitivas ou não consensuais de suas funções cerebrais, protegendo-os contra manipulações mentais através de tecnologias avançadas.
- Direito à Autonomia Mental: Essencial para assegurar que cada pessoa mantenha controle sobre suas próprias funções cognitivas e decisões, este direito defende a liberdade dos indivíduos de usar ou recusar tecnologias neurotecnológicas que possam alterar suas capacidades mentais.
- Direito à Proteção contra Viés Algorítmico e Discriminação: Este direito visa prevenir que algoritmos e outras tecnologias baseadas em inteligência artificial que interagem com dados cerebrais perpetuem preconceitos ou discriminem, assegurando uma interação tecnológica justa e igualitária.

Esses direitos visam garantir que as tecnologias neurotecnológicas sejam utilizadas de maneira ética, respeitando a dignidade e a liberdade dos indivíduos.

A privacidade mental impede que pensamentos e informações internas dos indivíduos sejam acessados sem permissão, garantindo que a mente humana permaneça um espaço inviolável. O direito à identidade pessoal protege contra alterações indesejadas na personalidade, assegurando que neurotecnologias não possam manipular a essência do indivíduo, e o direito ao livre arbítrio garante que as

decisões dos indivíduos não sejam influenciadas de forma manipulativa por tecnologias, preservando a autonomia de escolha do indivíduo[39].

Na era digital, onde a coleta e uso de dados pessoais são onipresentes, será que os direitos, mencionados no parágrafo anterior, estão sendo devidamente respeitados? Tecnologias como interfaces cérebro-computador (BCIs) e outras formas de neurotecnologia têm o potencial de acessar informações profundamente pessoais e influenciar diretamente os processos cognitivos dos indivíduos. Sem regulamentações adequadas, essas tecnologias podem ser exploradas para fins comerciais ou políticos, colocando em risco a privacidade e a autonomia mental dos indivíduos[40].

Um exemplo recente dessa vasta coleta de dados é o uso indevido de dados pessoais pela Meta para fins de treinamento de inteligência artificial, onde, recentemente, a Meta notificou milhões de europeus sobre uma nova alteração em sua política de privacidade. Uma análise mais detalhada dos links fornecidos na notificação revelou que a empresa pretende utilizar anos de postagens pessoais, fotos privadas e dados de rastreamento online para uma "tecnologia de inteligência artificial" não especificada, capaz de obter informações pessoais de qualquer fonte e compartilhá-las com "terceiros" não especificados. Em vez de solicitar o consentimento explícito dos usuários (*opt-in*), a Meta alega ter um interesse legítimo que prevalece sobre o direito fundamental dos europeus à proteção de dados e à privacidade. Além disso, uma vez que os dados são incorporados ao sistema, os usuários

[39] Orias, “Los neuroderechos”
[40] Orias, “Los neuroderechos”

não parecem ter a opção de removê-los (direito ao esquecimento - contexto europeu e direito ao apagamento dos dados)[41].

Max Schrems, advogado de privacidade e presidente honorário da Noyb, em relação a esse caso, afirmou o seguinte:

> A Meta basicamente afirma que pode usar 'quaisquer dados de qualquer fonte para qualquer finalidade e disponibilizá-los para qualquer pessoa no mundo', desde que seja feito usando 'tecnologia de IA'. Isto é claramente o oposto da conformidade com o GDPR. ""IA" é um conceito extremamente amplo. Assim como "usar dados em bancos de dados", não tem restrições legais. A meta não diz para que usará os dados, então pode ser um simples chatbot, uma publicidade personalizada extremamente agressiva , ou mesmo um drone assassino. Meta também afirma que os dados do usuário podem ser compartilhados com qualquer "terceiro" – o que significa qualquer pessoa no mundo[42].

A decisão da Meta de utilizar anos de postagens pessoais, fotos privadas e dados de rastreamento online para alimentar uma tecnologia de inteligência artificial não especificada compromete o direito à privacidade, incluindo a privacidade, que em última análise protege os indivíduos contra o acesso não autorizado a seus dados cerebrais e neurológicos. A coleta massiva e o processamento desses dados podem revelar pensamentos, intenções e comportamentos de maneira que os usuários não autorizaram explicitamente, violando a privacidade mental deles[43].

No Brasil, sobre esse caso, a ANPD determinou que a Meta interrompa imediatamente o uso de dados pessoais de seus usuários para o treinamento de

[41] "Noyb urges 11 DPAs to immediately stop Meta's abuse of personal data for AI." Noyb, 2024. https://noyb.eu/en/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai
[42] "Noyb urges 11 DPAs to immediately stop".
[43] Orias, "Los neuroderechos"

sistemas de inteligência artificial. Essa medida emergencial foi tomada após a Meta atualizar sua política de privacidade, ampliando as possibilidades de utilização dos dados, como já mencionado. Caso a empresa não cumpra a determinação, será aplicada uma multa diária de R$ 50 mil. A decisão visa proteger os dados de 102 milhões de usuários, evitando que sejam utilizados para esses fins sem a devida autorização[44].

A decisão da ANPD que proíbe a Meta de utilizar dados de usuários brasileiros para o treinamento de sistemas de inteligência artificial levanta preocupações sobre o uso ético de dados pessoais. Isso está diretamente relacionado ao conceito de neurodireitos, que visa proteger a privacidade mental e a autonomia dos indivíduos. Quando plataformas digitais utilizam dados pessoais de forma massiva e sem transparência para alimentar sistemas de IA, há o risco de que essas práticas interfiram não apenas na privacidade tradicional, mas também na privacidade mental.

Os neurodireitos, portanto, devem ser considerados na discussão sobre *dark patterns*, pois ambas as questões estão profundamente interligadas. O *design* embusteiro, ao manipular a tomada de decisões dos usuários através de *design*s enganosos e práticas de interface, podem comprometer a privacidade mental, a integridade psicológica e a autonomia mental dos indivíduos, que são os pilares dos neurodireitos, buscando sempre garantir que o desenvolvimento e a aplicação dessas tecnologias respeitem a dignidade e os direitos fundamentais dos indivíduos.

[44] "Após pedido de reconsideração, ANPD mantém Medida Preventiva aplicada à Meta." Ministério da Justiça e Segurança Pública, 2024. https://www.gov.br/anpd/pt-br/assuntos/noticias/apos-pedido-de-reconsideracao-anpd-mantem-medida-preventiva-aplicada-a-meta)

A crescente incorporação de neurotecnologias, como as Interfaces Cérebro-Computador (BCIs) e outras ferramentas que se conectam diretamente ao cérebro humano, oferece tanto benefícios quanto riscos consideráveis. Essas tecnologias têm o potencial de transformar tratamentos médicos e aumentar as capacidades humanas, mas também apresentam desafios significativos à privacidade mental, autonomia e integridade cognitiva. Isso exige uma resposta ética e legal forte e bem estruturada[45].

Dessa forma, pode-se notar que neurodireitos e a privacidade dos usuários estão intimamente conectados, a seguir seguem alguns exemplos de neurotecnologias:

- Interfaces Cérebro-Computador (BCIs): são sistemas que estabelecem uma comunicação direta entre o cérebro humano e um dispositivo externo. BCIs capturam sinais cerebrais e os traduzem em comandos que podem ser usados para controlar computadores, próteses robóticas e outros dispositivos eletrônicos. Exemplo: uma aplicação notável de BCIs é o controle de próteses robóticas por pessoas com paralisia. Por meio de eletrodos implantados no cérebro ou colocados no couro cabeludo, os sinais cerebrais podem ser capturados e usados para mover uma prótese, permitindo que os indivíduos realizem tarefas cotidianas de forma mais independente[46].

[45] Rainey, Stephen, Kevin McGillivray, Simi Akintoye, Tyr Fothergill, Christoph Bublitz, Bernd Stahl. “Desafios éticos e legais das neurotecnologias: uma análise crítica.” Journal of Law and the Biosciences, 7, no. 1, 2020. https://academic.oup.com/jlb/article/7/1/lsaa051/5864051?login=false

[46] Ramadas, Lucas Sérvio Gonçalves; “Os padrões obscuros “Dark Patterns” no e-commerce brasileiro.” Dissertação de Mestrado, Institutto brasileiro de ensino, pesquisa e desenvolvimento, Brasília, 2023.

- Realidade Virtual e Aumentada: Tecnologias de realidade virtual (VR) e realidade aumentada (AR) que interagem com o cérebro para criar experiências imersivas. Exemplo: na reabilitação neuropsicológica, a VR é usada para criar ambientes simulados onde os pacientes podem praticar habilidades motoras e cognitivas em um ambiente controlado e seguro. A AR, por outro lado, pode ser utilizada para fornecer informações adicionais em tempo real durante procedimentos cirúrgicos, melhorando a precisão e a segurança[47].

- Implantes Neurais: dispositivos implantados no cérebro para monitorar ou influenciar a atividade neural. Exemplo: Implantes neurais como o "Neuralink", desenvolvido pela empresa de mesmo nome, visam estabelecer uma interface direta entre o cérebro e computadores, permitindo não apenas o controle de dispositivos, mas também a potencial comunicação entre cérebros humanos e máquinas. Esses implantes têm o potencial de revolucionar a forma como interagimos com a tecnologia e como tratamos doenças neurológicas[48].

Os exemplos anteriormente citados demonstram que a proteção dos neurodireitos e a privacidade dos usuários estão intimamente conectadas, exigindo regulamentações robustas para garantir que o desenvolvimento e a aplicação dessas tecnologias respeitem a dignidade e os direitos fundamentais dos indivíduos.

---

https://repositorio.idp.edu.br/bitstream/123456789/4901/1/Dissertação_LUCAS%20SÉRVIO%20GONÇALVES%20RAMADAS_Mestrado_2023.pdf

[47] Orias, “Los neuroderechos”

[48] Ramadas, “Os padrões obscuros “Dark Patterns””

A questão dos *dark patterns* ou padrões obscuros se torna especialmente relevante no contexto do direito consumerista no Brasil, onde o Código de Defesa do Consumidor (CDC) já reconhece e protege a vulnerabilidade dos consumidores, inclusive no ambiente digital. Isso levanta um importante debate sobre o possível conflito entre essas práticas manipulativas e as proteções previstas no CDC, uma vez que os consumidores, muitas vezes, não compreendem plenamente as implicações das suas interações *online*, o que pode resultar em uma violação dos seus direitos fundamentais à informação clara e adequada.

A tese de Mariana de Moraes Palmeira[49] e a questão dos padrões obscuros (*dark patterns*) têm uma conexão intrínseca, especialmente quando se trata da vulnerabilidade dos consumidores no ambiente digital. Ambos os temas lidam com a manipulação de informações e a falta de transparência na coleta e uso de dados pessoais, que podem levar a uma exploração dos direitos dos indivíduos.

A vulnerabilidade digital é o foco central da tese de Palmeira[50], apontando para a exposição dos consumidores a práticas abusivas e a sua posição de hipossuficiência diante das grandes corporações tecnológicas. A autora argumenta que, na era do capitalismo de vigilância, onde a informação é um ativo crucial, os consumidores muitas vezes não têm o conhecimento ou os recursos necessários para se proteger contra a exploração de seus dados pessoais.

Assim sendo, fica evidenciado que as *dark patterns* são uma forma de manipulação digital que pode exacerbar a vulnerabilidade dos consumidores, especialmente quando se trata de dados pessoais sensíveis, como dados neurais. Em um

[49] Palmeira, "UX: entre o Marketing"
[50] Palmeira, "UX: entre o Marketing"

contexto em que neurotecnologias são cada vez mais utilizadas, há um risco significativo de que interfaces sejam projetadas para induzir os usuários a consentirem com a coleta de dados neurais sem compreender plenamente as implicações ou que talvez eles não tenham autonomia e tampouco conhecimento de quais dados efetivamente estão sendo coletados. Essa manipulação não apenas compromete a privacidade e a autodeterminação informacional dos indivíduos, mas também pode interferir em direitos fundamentais relacionados à integridade mental e ao livre arbítrio, que são centrais nos neurodireitos.

A conexão entre padrões obscuros e neurodireitos se torna especialmente preocupante quando consideramos que dados neurais podem revelar informações extremamente íntimas e sensíveis sobre pensamentos, emoções e estados mentais.

Reitera-se então, que, *designs* enganosos podem impactar não apenas dados pessoais tradicionais, mas também dados neurais, aumentando a vulnerabilidade digital dos indivíduos exigindo, assim, uma abordagem ética e jurídica robusta para garantir a proteção de neurodireitos.

Neurodireitos e proteção de dados: uma comparação entre Europa, Brasil, Chile e Estados Unidos

O avanço das neurotecnologias, como interfaces cérebro-computador e implantes neurais, traz à tona questões complexas sobre a proteção de dados pessoais e a integridade mental, demandando uma abordagem regulatória robusta e multifacetada. Neste contexto, a União Europeia, Brasil, Chile e Estados Unidos têm desenvolvido marcos legais distintos para enfrentar esses desafios. Enquanto a União Europeia se apoia no rigor do GDPR para proteger dados sensíveis, o Brasil avança com a consolidação da cultura que a LGPD implementou, que, embora inspirada

no GDPR, e mesmo já em vigor há alguns anos, ainda está em fase de evolução. O Chile, pioneiro na inclusão de neurodireitos em sua Constituição, estabelece um precedente global, enquanto os Estados Unidos começam a explorar a proteção de dados neurais através de legislações estaduais. Este tópico analisa como cada uma dessas jurisdições aborda a proteção dos neurodireitos e a privacidade dos usuários, comparando suas regulamentações e discutindo as implicações para o futuro da tecnologia e dos direitos humanos. Sendo:

- Proteção de Dados na União Europeia (GDPR): A proteção de dados na União Europeia é regida pelo Regulamento Geral sobre a Proteção de Dados (GDPR), que entrou em vigor em 25 de maio de 2018. Este regulamento estabelece um marco abrangente para a proteção de dados pessoais, com foco na transparência, controle e consentimento dos indivíduos sobre o uso de seus dados. O GDPR abrange não apenas dados convencionais, como nome e endereço, mas também dados sensíveis, incluindo dados biométricos e de saúde, que podem incluir dados neurais no futuro, dependendo da evolução tecnológica e das interpretações legais. O GDPR impõe obrigações rigorosas às empresas que processam dados pessoais, incluindo a exigência de bases legais claras para o processamento, o direito ao acesso e à portabilidade dos dados, e o direito ao esquecimento[51]. Uma característica central do GDPR é a proteção explícita de dados sensíveis, que são sujeitos a um nível mais elevado de proteção devido à sua natureza potencialmente prejudicial. No contexto de neurotecnologias, como interfaces cérebro-computador e implantes

[51] GDPR – General Data Protection Regulation. “Regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016.”, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

neurais, o GDPR pode ser interpretado para incluir dados neurais como dados sensíveis, exigindo medidas de proteção adicionais, como a minimização de dados e a realização de avaliações de impacto sobre a proteção de dados (DPIAs). Além disso, o GDPR prevê sanções severas para violações, com multas que podem atingir até 4% do faturamento global anual da empresa infratora, o que demonstra a seriedade com que a União Europeia trata a proteção dos dados pessoais dos seus cidadãos[52].

- Proteção de Dados no Brasil (LGPD): No Brasil, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, regulamenta o tratamento de dados pessoais e foi inspirada em grande parte pelo GDPR. A LGPD entrou em vigor em setembro de 2020 e trouxe uma nova era de responsabilidade no tratamento de dados pessoais no Brasil, estabelecendo princípios como a transparência, a finalidade específica, a adequação, e a necessidade, similares aos do GDPR. A LGPD também define dados sensíveis e os coloca sob uma camada adicional de proteção, incluindo dados relacionados à saúde, origem racial ou étnica, orientação sexual, e opiniões políticas, entre outros. No contexto brasileiro, dados neurais poderiam ser considerados como dados sensíveis sob a LGPD, especialmente em aplicações neurotecnológicas que envolvem informações de saúde ou biométricas[53]. A LGPD introduziu o conceito de "autodeterminação informativa", que reforça o controle dos indivíduos sobre seus próprios dados. Assim como o GDPR, a LGPD exige o consentimento livre, específico e em destaque, que seja de fácil entendimento do titular, para o tratamento de dados sensíveis, o que seria essencial no caso de

[52] GDPR. “Regulation (EU) 2016/679 of the european parliament.”
[53] “Lei nº 13.709, de 14 de Agosto de 2018

dados neurais capturados por interfaces cérebro-computador ou outras neurotecnologias. O Brasil também está implementando uma estrutura de governança robusta através da Autoridade Nacional de Proteção de Dados (ANPD), que supervisiona e atualiza a aplicação da LGPD e garante que as práticas de tratamento de dados sejam alinhadas aos princípios estabelecidos na lei.

- Abordagens de Proteção de Neurodireitos nos Dois Contextos: A proteção de neurodireitos, um campo emergente que busca proteger os direitos fundamentais em face das neurotecnologias, tem ganhado atenção tanto na Europa quanto no Brasil. No contexto europeu, embora o GDPR não mencione explicitamente os neurodireitos, as proteções conferidas a dados sensíveis e biométricos podem ser estendidas a dados neurais. A proteção rigorosa do GDPR e sua aplicação universal na UE fornecem uma base sólida para a proteção dos neurodireitos, assegurando que qualquer tratamento de dados neurais seja realizado com alto nível de cuidado e respeito pela dignidade humana[54]. No Brasil, a discussão sobre neurodireitos ainda está em desenvolvimento, mas a LGPD já oferece um quadro legal que pode ser aplicado à proteção de dados neurais. Considerando que a LGPD trata os dados sensíveis com um nível de proteção elevado, qualquer avanço em neurotecnologias precisaria se alinhar com esses requisitos. Ainda, está tramitando no congresso uma proposta de ementa à Constituição que se aprovada, irá incluir, entre os direitos e garantias fundamentais, a proteção à integridade

[54] Ienca, Andorno, “Towards new human rights”

mental e a transparência algorítmica que seriam neurodiretos[55]. Além disso, o Brasil tem mostrado interesse em seguir as tendências internacionais de proteção de dados, o que poderia incluir a incorporação explícita dos neurodireitos em futuras revisões legislativas ou regulatórias, o que já está acontecendo através da proposta de emenda à Constituição[56].

- Legislação de Neurodireitos no Chile e nos Estados Unidos: o Chile se tornou o primeiro país do mundo a legislar especificamente sobre neurodireitos. Em 2021, o país aprovou uma reforma constitucional que reconhece os neurodireitos como direitos fundamentais, inserindo no artigo 19 da Constituição Chilena a proteção à integridade mental e a garantia de que tecnologias que interfiram na mente humana sejam utilizadas de forma a respeitar a dignidade e a autonomia das pessoas. Essa legislação pioneira destaca a importância de proteger os dados neurais e prevenir a manipulação mental, estabelecendo um precedente para outros países[57].

- Legistalção dos Estados Unidos: embora ainda não exista uma legislação federal consolidada sobre neurodireitos, houve progressos significativos. Em abril de 2024, foi promulgada uma lei no estado do Colorado que classifica

[55] "Proposta de Emenda à Constituição n° 29, de 2023." Senado Federal,2023. https://legis.senado.leg.br/sdleg-getter/documento?dm=9386704&ts=1686688862951&disposition=inline

[56] Tepedino, Gustavo, Ana Frazão, Milena Donato Oliva. "Lei geral de proteção de dados pessoais: e suas repercussões no direito brasileiro." Superior Tribunal de Justiça, Revista dos tribunais, 2023. https://bdjur.stj.jus.br/jspui/bitstream/2011/139297/lei_geral_protecao_tepedino_3.ed.pdf

[57] Yuste, Rafael, Jared Genser & Stephanie Hermann. "It's time for neuro-rights." Horizons Journal of International Relations and Sustainable development, n. 18, 2021,. https://www.perseus-strategies.com/wp-content/uploads/2021/03/Neuro-Rights-Horizons-Winter-2021.pdf

dados neurais como dados sensíveis, impondo restrições rigorosas sobre seu tratamento, especialmente em contextos comerciais. Essa legislação reflete a crescente preocupação com a privacidade e a integridade mental em um ambiente de rápido avanço tecnológico[58].

A principal diferença entre os contextos europeu, brasileiro, chileno e americano está na maturidade e na aplicação prática das regulações. Enquanto a Europa já possui um histórico robusto de aplicação do GDPR, com várias decisões judiciais moldando a interpretação e a aplicação da lei, o Chile se destaca pela legislação específica sobre neurodireitos, e os Estados Unidos estão dando os primeiros passos com legislações estaduais. No entanto, todos esses contextos mostram um compromisso crescente com a proteção de dados pessoais e neurodireitos, fundamentais em um futuro dominado por tecnologias avançadas[59] [60].

3. Conclusão

Este artigo teve como objetivo explorar as implicações dos *dark patterns* na privacidade dos usuários, comparando as regulamentações europeias e brasileiras, além de discutir a interseção entre essas práticas de *design* manipulativas e os neurodireitos. A análise revelou que, enquanto o GDPR e a LGPD oferecem bases sólidas para a proteção de dados sensíveis, há desafios específicos quando se trata de práticas que exploram vulnerabilidades, como as de crianças, adolescentes e usuários expostos a neurotecnologias. Esses grupos, em particular, demandam uma

[58] Pilato, Ana Julia. Primeira lei de privacidade de ondas cerebrais é aprovada nos EUA. Olhar digital, 2024. https://olhardigital.com.br/2024/04/23/seguranca/primeira-lei-de-privacidade-de-ondas-cerebrais-e-aprovada-nos-eua/
[59] Ienca, Andorno, “Towards new human rights”
[60] Yuste, “It’s time for neuro-rights”

proteção regulatória mais robusta e específica, capaz de lidar com a manipulação digital em interfaces que podem impactar não apenas suas decisões, mas também sua integridade mental.

As questões éticas emergem como um aspecto central nesse contexto, especialmente no que diz respeito à manipulação deliberada dos usuários por meio de *design* enganosos. A falta de transparência nas interfaces digitais e nos algoritmos que governam essas interações compromete o direito dos usuários de tomar decisões informadas e voluntárias. A transparência algorítmica, talvez seja de vital importância para garantir que as práticas de *design* sejam orientadas por princípios éticos e que os usuários tenham a clareza necessária para compreender como seus dados são coletados, processados e utilizados.

Além disso, a crescente adoção de neurotecnologias, como interfaces cérebro-computador e implantes neurais, acrescenta uma camada adicional de complexidade. Essas tecnologias têm o potencial de acessar e manipular dados neurais, exigindo que as regulamentações de proteção de dados evoluam para incluir salvaguardas específicas para neurodireitos. As questões éticas e práticas de auditoria de algoritmo, nesse cenário, tornam-se necessárias, pois os algoritmos que processam dados neurais devem ser desenvolvidos e utilizados de forma a garantir que não ocorram abusos ou violações da integridade mental dos indivíduos.

Este estudo destacou a necessidade urgente de uma abordagem ética no *design* de interfaces e de regulamentações que assegurem a dignidade e os direitos fundamentais dos indivíduos em um ambiente digital cada vez mais intrusivo. Portanto, é essencial que os reguladores, desenvolvedores e legisladores atuem de maneira coordenada, garantindo que os avanços tecnológicos respeitem os limites éticos e promovam a transparência, assegurando a confiança e a proteção dos usuários.

Referências bibliográficas

Acquisti, Alessandro, Laura Brandimarte & George Loewenstein. "Privacy and human behavior in the age of information." Science, 347(6221), 509-514, 2015.
Bösch, Christoph, Benjamin Erb, Frank Kargl, Henning Kopp & Stefan Pfattheicher. "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns." Proceedings on Privacy Enhancing Technologies, 2016(4), 237-254. https://www.researchgate.net/publication/303814886_Tales_from_the_Dark_Side_Privacy_Dark_Strategies_and_Privacy_Dark_Patterns
Brandão, Renan Sancho. "Tratamento de dados pessoais de crianças e adolescentes: análises e perspectivas." Monografia, Universidade Federal do Rio de Janeiro, 2022. https://pantheon.ufrj.br/handle/11422/19142
Brignull, Harry. "Dark Patterns: Deception vs. Honesty in UI Design". 2011. https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/
Dark patterns in data protection, Lickslegal, 2023, https://www.lickslegal.com/post/dark-patterns-in-data-protection
Eberlin, Fernando Büscher von Teschenhausen. "Proteção de dados pessoais da criança: privacidade, vulnerabilidade e consentimento na sociedade da informação." Dissertação de Mestrado, Universidade Presbiteriana Mackenzie, 2019. https://bdtd.ibict.br/vufind/Record/UPM_27ce6ed381aa9f5fb0a3fd2e271e3ffa
Faraoni, Stefano. "Persuasive Technology and Computational Manipulation: Hypernudging out of Mental Self-Determination." Frontiers in Artificial Intelligence, 6, 2023. https://doi.org/10.3389/frai.2023.1216340
GDPR – General Data Protection Regulation. "Regulation (EU) 2016/679 of the european parliament and of the council of 27 April 2016", 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
Gray, Colin M., Yubo Kou, Bryan Battles, Joseph Hoggatt, & Autin L. (2018). "The dark (patterns) side of UX design." Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 534.
Henriques, Isabella Vieira Machado, Inês Vitorino Sampaio. "Discriminação algorítmica e inclusão em Sistemas de Inteligência Artificial – uma reflexão sob a ótica dos direitos da criança no ambiente digital". RDB, Brasília, 18, no. 100 (out. dez. 2021): 245-271. https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5993/pdf
Ienca, Marcello; Roberto Andorno. "Towards new human rights in the age of neuroscience and neurotechnology." Life Sciences, Society and Policy, 13, no. 5, 2017. https://link.springer.com/article/10.1186/s40504-017-0050-1
Kelly, Samantha Murphy. "Nova York processa redes sociais por crise de saúde mental de adolescentes." CNN Brasil, 2024. https://www.cnnbrasil.com.br/economia/negocios/nova-york-processa-redes-sociais-por-crise-de-saude-mental-de-adolescentes/

Lei nº 13.709, de 14 de Agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). Diário Oficial da União, 15 de agosto de 2018, seção 1, p. 53-58.
Luguri, Jamie, & Lior Jacob Strahilevitz. "Shining a Light on Dark Patterns". Journal of Legal Analysis, 13, 43-109, 2023.
Mathur, Arunesh, Gunes Acar, Michael Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, & ArvindNarayanan, A. (2019). "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites". Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 81, 2019. https://dl.acm.org/doi/10.1145/3359183
Mazumdar, Stuti & Symran Bhue. "Responsible design part 10 of 14 : privacy zuckering." Thing Design, 2022. https://think.design/blog/responsible-design-part-10-of-14-privacy-zuckering/#:~:text=Privacy%20Zuckering%20is%20a%20dark,the%20users%20had%20intended%20to
Noyb urges 11 DPAs to immediately stop Meta's abuse of personal data for AI. Noyb, 2024. https://noyb.eu/en/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai
Orias, Ramiro. "Los neuroderechos: una nueva Frontera para los Derechos Humanos." Agenda Internacional, Año XXIX, no. 40, 2022, 211-227. https://revistas.pucp.edu.pe/index.php/agendainternacional/article/view/26019/24500
Palmeira, Mariana de Moraes. "UX: entre o Marketing e a Lei Geral de Proteção de Dados (LGPD)." Observatório da Comunicação, 2020. https://observatoriodacomunicacao.org.br/artigos/ux-entre-o-marketing-e-a-lei-geral-de-protecao-de-dados-lgpd-por-mariana-de-moraes-palmeira/
Proposta de Emenda à Constituição n° 29, de 2023. Senado Federal,2023. https://legis.senado.leg.br/sdleg-getter/documento?dm=9386704&ts=1686688862951&disposition=inline
Ramadas, Lucas Sérvio Gonçalves; "Os padrões obscuros "Dark Patterns" no e-commerce brasileiro." Dissertação de Mestrado, Institutto brasileiro de ensino, pesquisa e desenvolvimento, Brasília, 2023. https://repositorio.idp.edu.br/bitstream/123456789/4901/1/Disserta%C3%A7%C3%A3o_LUCAS%20S%C3%89RVIO%20GON%C3%87ALVES%20RAMADAS_Mestrado_2023.pdf
Tepedino, Gustavo, Ana Frazão, Milena Donato Oliva. "Lei geral de proteção de dados pessoais: e suas repercussões no direito brasileiro." Superior Tribunal de Justiça, Revista dos tribunais, 2023. https://bdjur.stj.jus.br/jspui/bitstream/2011/139297/lei_geral_protecao_tepedino_3.ed.pdf
Yuste, Rafael, Jared Genser & Stephanie Hermann. "It's time for neuro-rights." Horizons Journal of International Relations and Sustainable development, n. 18, 2021,. https://www.perseus-strategies.com/wp-content/uploads/2021/03/Neuro-Rights-Horizons-Winter-2021.pdf